



virtually anyone including service providers, system operators, third party vendors and end-users.

To permit adaptation of newly developed functionality to the communication network, and/or to permit utilization of external network functionality by users of the communication network, it is necessary to interface the new functions to the communication network in a stable and secure manner.

Thus, there is a need for a method and apparatus for interfacing a network to an external element in a stable and secure manner.

#### Brief Description of the Drawings

FIG. 1 is a block diagram illustration of a communication network coupled to an external element by an apparatus in accordance with a preferred embodiment of the present invention.

FIG. 2 is a functional block diagram illustrating the interface of an external element to a communication network in accordance with a preferred embodiment of the present invention.

FIG. 3 is a functional block diagram illustration of a services delivery element in accordance with a preferred embodiment of the invention.

FIG. 4 is a functional block diagram of a services delivery element in accordance with one of the preferred embodiments of the invention illustrating further functionality of the services delivery element.

FIG. 5 is a functional block diagram illustrating services invocation between a communication network and an external element in accordance with one of the preferred embodiments of the present invention.

FIG. 6 is a block diagram illustration of a communication network coupled to an external element by an apparatus in accordance with a preferred embodiment of the present invention.

5

#### Detailed Description of the Preferred Embodiments

A services delivery element forms an interface or operates as an interface device between an external element (such as an external end user's network feature server) and a communication network including both a core network and at least one access network. The services delivery element provides access to the core network, access networks and subscriber devices within or connected to the access networks to which the external element is interfaced. In accordance with a first aspect of the invention, the services delivery element acts as a security proxy and a secure link point between the external element and the core network. The services delivery element may also provide managed access by the external element to core network and access network resources. In addition to the above-described features, the services delivery element may also recognize or identify trusted external elements; identify preferential external elements; provide secure access to subscriber data retained within the core network; identify and deny access by untrusted external elements; translate between the external element and the core network; and provide limited access to particular subsets of core network data and/or functions by the external element.

With reference to FIG. 1, a core network 10 is interfaced to an access network 12. The core network 10 may be a packet based communication network adapted to provide voice and data communication services via the

access network 12, which may be a radio access network. A radio access network provides wireless voice and data communication services to a mobile unit, such as the mobile unit 14, and may do so in accordance with virtually any wireless communication protocol. The invention provides an interface for external elements to both the core network 10, the access network 12, and the mobile unit 14. To simplify the following discussion of the preferred embodiments of the invention, reference is made only to the core network 10.

Referring to FIG. 1 and FIG. 2, within the core network 10 is a variety of application program interfaces (API) 18, which interface services and functional components within the core network 10. As shown in FIG. 2, for example, is a call model API 19 and a resource API 20. Each of API 19 and API 20 are considered to be internal APIs, and as such have "trusted" status within the core network 10. That is, these APIs have access to the core network 10 without having to first authenticate and establish a secure interface with the core network. Also illustrated in FIG. 2 are external APIs 22, such as applications API 23 and services API 24. While only two external APIs 23 and 24 are shown, it should be understood that numerous external APIs might be provided.

External APIs 22 are considered "untrusted" APIs and do not have the same, direct access to the core network 10 as the trusted, internal APIs 18. The internal APIs 18 may be considered the "glue" of core network 10, which enable the features and services in the core network 10. As an example, the internal APIs support the configuration of the communication between the network entities (not shown) within the core network 10.

In contrast, the external APIs 22 are accessible to and configurable by third parties, e.g., services providers and, where appropriate, end users. The external APIs 22 are the feature extraction pieces that enable third party  
5 developers to access and add features and services to the network. The external APIs 22 interface with the internal APIs 18 to configure, communicate with and control the network to provide extensibility to the core network 10. In accordance with a preferred embodiment of the invention,  
10 the external APIs 22 and internal APIs 18 are linked together via a services delivery element 26. The services delivery element 26 segregates the sets of APIs, and has a primary purpose to provide security for the internal APIs from untrusted resources.

15 Because the external APIs 22 connect to the core network 10, it is possible that mechanisms may be added to the core network 10 via these external APIs 22, that can be damaging or even totally destructive. Any service, not resident within the core network 10, that requires the  
20 execution of programmable code, that requires processing from a core network entity, or data access on behalf of a subscriber from the core, is considered external. These services, such as the Call Processing Language from the IPTEL working group of the Internet Engineering Task Force  
25 (IETF) or some features of the Wireless Application Protocol(WAP), enable end users to load executable code into the network. These services cannot be trusted and should not be granted direct access to the core network 10.

30 As discussed above, the internal APIs 18 are the system interfaces which enable features and services in the core network 10. The internal APIs 18 address the configuration of and communication between the network

entities inside both the core and access networks 10 and 12. These interfaces will not be directly accessible external to the core network 10.

The services delivery element 26 protects the core network 10 from potentially destructive features and services, and further provides indirect access to the internal APIs 18. FIG. 3 illustrates a functional architecture for the services delivery element 26 in accordance with a preferred embodiment of the invention.

The services delivery element 26 may include both a security services element 302 and a translation/API modules element 304. One of ordinary skill in the art will appreciate that FIG. 3 represents the functional elements of the services delivery element 26, and that in an actual physical embodiment of the services delivery element 26, these functional elements may reside in one or more components of the core network 10.

The security services element 302 provides authentication and validation services to potential service and feature providers of the network. In accordance with the preferred embodiments of the invention, access to the core network 10 by external elements, i.e., external APIs 22, are via a secure connection across a virtual private network (VPN) connection. The security services element 302 adds a wrapper on top of the internal API that will enable the external feature or service. This arrangement allows the external feature or service to have scalable access to the internal API 18, but through a secure technique. Access to the internal API 18 by the external elements ranges from no access to partial access to full access based on a variety of security variables. These variables include user based privileges (e.g., service

options based on subscription information) and network variables (e.g., based on network usage and load). More generally speaking, the services delivery element 26 enables a layering of restrictions providing greater or lesser authorization to the external element based upon virtually any set of criteria, including without limitations those set forth above.

The connection security between the external API 22 and the internal API 18 may be provided using the IP security protocol (IPSec) from the Internet Engineering Task Force (IETF). Utilizing both the encapsulation payload (ESP) and authentication header (AH) services of IPSec, the security delivery element 26 will provide access control, connectionless integrity, data origin authentication, rejection of replayed packets, and confidentiality services. These services will be available for both TCP and UDP streams.

The services delivery element 26 may be configured to communicate in IPSec tunnel mode. In this mode of operation, both the external API 22 and the internal API 18 will authenticate and encrypt the entire IP source packet and wrap a new IP header around them. ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header. AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Since, as described, the services delivery element 26/ external API 22 IPSec transmissions will be in tunnel mode, all of the hosts inside the core network 10 will communicate with the external API 22 without implementing IPSec. The unprotected packets generated by core network elements are tunneled through the services delivery element

26 by tunnel security associations. The internal APIs 18 may interact with the services delivery element 26 via the embedded security layer on the services delivery element 26. This level of security is implemented to authenticate and validate each particular external API 22.

In accordance with the preferred embodiments of the invention, the services delivery element 26 may be configured to recognize particular external APIs 22. For example, one third party vendor may have more access to the core network 10 than others. Such recognition may be based upon being a known services provider, type of service, or other criteria. Establishing such other criteria will be easily recognized by one having ordinary skill in the art. In this arrangement, the services API 24 will interact with the services delivery element 26 via the embedded Security Layer on the security delivery element 26. This level of security is implemented to authenticate and validate each particular external element, and provide an explicit security layer between the external elements and the core network 10.

External elements (e.g., Feature Server 606 (FIG. 6)) accessing the system via the External APIs 22 may be statically or dynamically associated with the core network 10. For external services that are expected to be delivered to numerous subscribers the operator may configure the core network 10 so that the external API 22 associated with the external service remains statically connected to the core network 10 via this security technique at system initialization. In a dynamic case, when a subscriber requests a particular feature provided by an external element, the core network 10 interrogates the external element.

The associated external API 22 registers with the service delivery element 26, and the services delivery element 26 will authenticate the external element and grant the particular external API 22 access privileges based on this authentication. At this point the external element becomes a trusted element by obtaining the security information. This implies that an additional layer of software must be considered in addition to the external API 22 or that the external API 22 has a local component, which adds the security parameter. A failed security check results in the call to the external API 22 returning an exception.

It will be appreciated that the service delivery element 26 may apply additional or alternate treatments in the event of a failed security check. The treatment applied may depend on the context of the security check failure. For example, a service usage accounting record may be created for the attempted service request. The record could be populated with specific information regarding the attempt and the reason for the security check failure, i.e., the denial of services. In the event the incoming request involves an external caller trying to reach the mobile unit 14 or access data held within the service delivery element 26, additional treatments may be applied. By way of example, an external caller attempting to access the mobile unit 14, but denied access, may be connected to a recorded announcement or progress tone to convey the reason that the access was not granted. The external caller might also be directed to a web page to provide additional information about the failed access attempt.

The foregoing arrangement is illustrated in FIG. 4. An external feature server 402 and its associated services API 404 are coupled via a message layer 406 to a security layer 408. The security layer 408 interfaces via the  
5 external services API 24 to the services delivery element 26.

Once the external element is trusted to the services delivery element 26 a subscriber may attempt to access a given feature provided by the external element. At this  
10 point, the core network 10 has access to the external element 402 via its associated API 404 and the security delivery element 26, but the subscriber does not have direct access, i.e., security rights, to the feature offerings of the external element. The subscriber requests  
15 the feature and then the services delivery element 26 passes a token on behalf of the subscriber to the external element. The token exchange, shown pictorially in FIG. 5, occurs at the start of the service dialog to enable a particular feature server 502 and its associated services  
20 API 504 and the associated service data to support the feature. Service data may be subscriber data such as profile information, location data, etc. An access token 506 is passed between the external API 22 and the services API 504 containing the service request data. It will be  
25 appreciated that there may be multiple levels of security checks before this data can be delivered outside the core network 10.

The token exchange and associated authentication lasts for the duration of the dialogue. It should be noted that  
30 the dialogue might be a single service request or equivalent to a registration, which may persist over a number of hours. The first external API call establishes

-11-

the security relationship between the requestor and the external element. For the lifetime of the relationship, the subsequent external API calls are considered as being sourced by a trusted element. This assumes that the requestor has additional software to support the security check.

Once a security relationship has been established, an external element may need to gain access to additional resources or data within the core network 10. The service API 22 will allow an explicit renegotiation of the security relationship to expand the access granted the external element. This process may also be applied in a reverse fashion to limit the access granted to the external element. For long-lived security relationships, the relationship may be aged to ensure release of the relationship after a predetermined time. This time out period may also be combined with some other criteria, such as inactivity. Once the time out period has expired the external element would be required to re-establish its secure relationship as described herein.

Because services are being provided by external elements, each external element may not use a protocol that is entirely compatible with the internal APIs and/or the core network 10. The services delivery element 26 includes translation functions 304 and API modules 306 (FIG. 3) that translate the service requests from external elements to the known internal API services. This translation function will operate similar to a broker function, a protocol adapter, or a protocol gateway function. The available services will be determined by the authentication services of the security services offered by the services delivery element 26. For example, Java Telephony Application

Interface (JTAPI) may be supported external to the core network 10 via a translation function 304 within the services delivery element 26. Other translation protocols that may be supported include PARLAY, Telephony Application Interface (TAPI), Java Advanced Intelligent Network (JAIN) and Telecommunication Information Networking Architecture (TINA), which are illustrated in FIG. 3.

The invention may be further illustrated by three use cases, of which two are illustrated in FIG. 6.

1. An external element 602 is hosted in the End User Services Network 604 co-located within the core network 10,
2. An external element 606 is located in or attached to a non-trusted, external network 608 such as the internet, and
3. An external element is located in a trusted or non-trusted external network such as a private service provider network (not shown in FIG. 6).

In the first case, the end-user services network 604 is a trusted entity in a trusted network within the core network 10. In this case the relationship implies a trusted external element accessible over a trusted link. The external element 602 is either imbedded in the trusted network or is represented as a trusted core network 10 entity. This case can be thought of as one where certain classes of services such as three-way voice calling, voice call forwarding, paging, electronic mail, and other "typical" services may be provisioned within the core network 10. As a result, trust is static and requires only service level access security per subscriber.

In the second case, the external element 606 resides in a network 608 attached to the Internet. In this case neither the link to the network 608 where the external element 606 resides

nor the external element 606 itself is considered trusted. A secure link 610 between the core network 10 and the Internet point of attachment to the packet gateway 612 of the core network 10 must first be established followed by secure access between the mobile unit 14 and the external element 606. As shown in FIG. 6, the mobile unit 14 is provided access to the core network 10 via a trusted element, the services client 614 internal to the core network 10. If there is need for access to resources contained within the core network 10, secure access via security associations 616 is established between the internal APIs 18 and the external element 606, which would automatically invoke the security services in the services delivery element 26. The reverse case, where the external element 606 attempts unsolicited contact with a mobile unit 14, would require the external element establish a secure link with the core network 10 followed by successful security negotiation with the internal API 18 for service discovery. This would be necessary for actions such as subscriber endpoint location and discovery of subscriber device attributes and/or capabilities.

In the third case, the external element resides in an external, trusted, private network. This allows statically or dynamically negotiated trust between networks and between an external element and the core network 10 internal APIs 18 to be negotiated jointly or independently using persistent (i.e., logically or physically) or short-lived link states.

The present invention has been described in terms of several preferred embodiments. It will be appreciated that the invention may be altered or changed without departing from its fair scope. For example, the invention may be applied where an external element, such as an external API, is utilized for remote configuration of elements associated with the core network. Such an implementation would find beneficial use in a system permitting subscriber profile provisioning from a device other than the subscriber device itself. The layered restrictions

[illegible]